G 0.45 Datenverlust

Ein Datenverlust ist ein Ereignis, das dazu führt, dass ein Datenbestand nicht mehr wie erforderlich genutzt werden kann (Verlust der Verfügbarkeit). Eine häufige Form des Datenverlustes ist, dass Daten unbeabsichtigt oder unerlaubt gelöscht werden, zum Beispiel durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware.

Ein Datenverlust kann jedoch auch durch Beschädigung, Verlust oder Diebstahl von Geräten oder Datenträgern entstehen. Dieses Risiko ist bei mobilen Endgeräten und mobilen Datenträgern häufig besonders hoch.

Weiterhin ist zu beachten, dass viele mobile IT-Systeme nicht immer online sind. Die auf diesen Systemen gespeicherten Daten befinden sich daher nicht immer auf dem aktuellsten Stand. Wenn Datenbestände zwischen mobilen IT-Systemen und stationären IT-Systemen synchronisiert werden, kann es durch Unachtsamkeit oder Fehlfunktion zu Datenverlusten kommen.

Beispiele:

- Das Smartphone fällt aus der Hemdtasche und zerschellt auf den Fliesen, ein Tablet wird statt der Zeitung vom Hund apportiert, leider mit Folgen. Solche und ähnliche Ereignisse sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Es gibt Schadprogramme, die gezielt Daten auf infizierten IT-Systemen löschen. Bei einigen Schädlingen wird die Löschfunktion nicht sofort bei der Infektion ausgeführt, sondern erst, wenn ein definiertes Ereignis eintritt, zum Beispiel wenn die Systemuhr ein bestimmtes Datum erreicht.
- Viele Internet-Dienste können genutzt werden, um online Informationen zu speichern. Wenn das Passwort vergessen wird und nicht hinterlegt ist, kann es passieren, dass auf die gespeicherten Informationen nicht mehr zugegriffen werden kann, wenn über den Internet-Dienst kein geeignetes Verfahren zum Zurücksetzen des Passwortes angeboten wird.
- Festplatten und andere Massenspeichermedien haben nur eine begrenzte Lebensdauer. Wenn keine geeigneten Redundanzmaßnahmen getroffen sind, kann es durch technische Defekte zu Datenverlusten kommen.

G 0.46 Integritätsverlust schützenswerter Informationen

Die Integrität von Informationen kann durch verschiedene Ursachen beeinträchtigt werden, z. B. durch Manipulationen, Fehlverhalten von Personen, Fehlbedienung von Anwendungen, Fehlfunktionen von Software oder Übermittlungsfehler.

- Durch die Alterung von Datenträgern kann es zu Informationsverlusten kommen.
- Übertragungsfehler: Bei der Datenübertragung kann es zu Übertragungsfehlern kommen.
- Schadprogramme: Durch Schadprogramme können ganze Datenbestände verändert oder zerstört werden.
- Fehleingaben: Durch Fehleingaben kann es zu so nicht gewünschten Transaktionen kommen, die häufig lange Zeit nicht bemerkt werden.
- Angreifende können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.
- Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.

Wenn Informationen nicht mehr integer sind, kann es zu einer Vielzahl von Problemen kommen:

- Informationen können im einfachsten Fall nicht mehr gelesen, also weiterverarbeitet werden.
- Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden. Hierdurch können beispielsweise Überweisungen in falscher Höhe oder an die falschen Empfangenden ausgelöst werden, die Absendeangaben von E-Mails könnten manipuliert werden oder vieles mehr.
- Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren (hier reicht die Änderung eines Bits), können sie unter Umständen nicht mehr entschlüsselt bzw. entpackt werden.
- Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.
- Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

IT-gestützte Angriffe können Auswirkungen haben, die

- von den Angreifenden nicht beabsichtigt sind oder
- nicht die unmittelbar angegriffenen Zielobjekte betreffen oder
- unbeteiligte Dritte schädigen.

Ursächlich hierfür sind die hohe Komplexität und Vernetzung moderner Informationstechnik sowie die Tatsache, dass die Abhängigkeiten der angegriffenen Zielobjekte und der zugehörigen Prozesse in der Regel nicht offenkundig sind.

Dadurch kann es unter anderem dazu kommen, dass der tatsächliche Schutzbedarf von Zielobjekten falsch eingeschätzt wird oder dass die Verantwortlichen für die Zielobjekte kein Eigeninteresse an der Behebung von Mängeln dieser Zielobjekte haben.

Beispiele:

- Auf IT-Systemen installierte Bots, mit denen die Angreifenden verteilte Denial-of-Service-Angriffe (DDoS-Angriffe) durchführen können, stellen für die infizierten IT-Systeme selbst oft keine direkte Gefahr dar, weil sich die DDoS-Angriffe in der Regel gegen IT-Systeme Dritter richten.
- Schwachstellen von IoT-Geräten in WLANs können von Tätern und Täterinnen als Einfallstor genutzt werden, um andere wichtigere Geräte im gleichen WLAN anzugreifen. Deshalb müssen solche IoT-Geräte auch dann geschützt werden, wenn sie selbst nur einen geringen Schutzbedarf haben.
- Ransomware-Angriffe auf IT-Systeme können unter Umständen Kettenreaktionen auslösen und damit auch Kritische Infrastrukturen treffen. Dies wiederum könnte zu Versorgungsengpässen der Bevölkerung führen, auch wenn die Angreifenden dies möglicherweise gar nicht beabsichtigt haben.

ISMS: Sicherheitsmanagement

Bundesamt
für Sicherheit in der
Informationstechnik

ISMS.1 Sicherheitsmanagement

1. Beschreibung

1.1. Einleitung

Mit (Informations-)Sicherheitsmanagement wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen jeder Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

1.2. Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, wie ein funktionierendes Managementsystem für Informationssicherheit (ISMS) eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Der Baustein beschreibt dazu Schritte eines systematischen Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines Sicherheitskonzeptes.

1.3. Abgrenzung und Modellierung

Der Baustein ISMS.1 *Sicherheitsmanagement* ist auf den Informationsverbund einmal anzuwenden.

Der Baustein baut auf den BSI-Standards 200-1 „Managementsysteme für Informationssicherheit“ und 200-2 „IT-Grundschutz-Methodik“ auf. Er fasst daraus die wichtigsten Aspekte zum Sicherheitsmanagement zusammen.

In der Institution sollten regelmäßig Sicherheitsrevisionen durchgeführt werden. Ausführliche Anforderungen dazu sind nicht in diesem Baustein, sondern im Baustein DER 3.1 *Audits und Revisionen* zu finden. Außerdem sollten alle Mitarbeitenden der Institution sowie alle relevanten Externen systematisch und zielgruppengerecht zu Sicherheitsrisiken sensibilisiert und zu Fragen der Informationssicherheit geschult werden. Ausführliche Anforderungen dazu sind im Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* zu finden.

Dieser Baustein behandelt ebenso keine spezifischen Aspekte zu Personal oder zum Bereich Organisation. Diese Anforderungen werden in den Bausteinen ORP.2 *Personal* bzw. ORP.1 *Organisation* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein ISMS.1 *Sicherheitsmanagement* von besonderer Bedeutung.

2.1. Fehlende persönliche Verantwortung im Sicherheitsprozess

Sind in einer Institution die Rollen und Zuständigkeiten im Sicherheitsprozess nicht eindeutig festgelegt, dann ist es wahrscheinlich, dass viele Mitarbeitende ihre Verantwortung für die Informationssicherheit mit dem Verweis auf übergeordnete Hierarchie-Ebenen ablehnen oder vergessen. Als Folge werden Sicherheitsmaßnahmen nicht umgesetzt, da diese zunächst fast immer einen Mehraufwand im gewohnten Arbeitsablauf darstellen.

2.2. Mangelnde Unterstützung durch die Institutionsleitung

Werden die Sicherheitsverantwortlichen nicht uneingeschränkt durch die Institutionsleitung unterstützt, kann es schwierig werden, die notwendigen Maßnahmen einzufordern. Dies gilt insbesondere für Personen, die in der Linienstruktur über den Sicherheitsverantwortlichen stehen. In diesem Fall ist der Sicherheitsprozess nicht vollständig durchführbar.

2.3. Unzureichende strategische und konzeptionelle Vorgaben

In vielen Institutionen wird zwar ein Sicherheitskonzept erstellt, dessen Inhalt ist dann aber häufig nur wenigen Personen in der Institution bekannt. Dies führt dazu, dass Vorgaben an Stellen, an denen organisatorischer Aufwand zu betreiben wäre, bewusst oder unbewusst nicht eingehalten werden.

Auch wenn das Sicherheitskonzept strategische Zielsetzungen enthält, werden diese von der Institutionsleitung vielfach als bloße Sammlung von Absichtserklärungen betrachtet. Häufig werden dann keine ausreichenden Ressourcen zur Umsetzung zur Verfügung gestellt. Oft wird fälschlicherweise auch davon ausgegangen, dass in einer automatisierten Umgebung Sicherheit automatisch hergestellt wird.

Ohne strategische Vorgaben wird bei Schadensfällen häufig unstrukturiert vorgegangen. Dadurch können bestenfalls Teilaspekte verbessert werden.

2.4. Unzureichende oder fehlgeleitete Investitionen

Wenn die Institutionsleitung nicht ausreichend über den Sicherheitszustand sämtlicher Geschäftsprozesse, IT-Systeme und Anwendungen sowie über vorhandene Mängel unterrichtet ist, werden nicht genügend Ressourcen für den Sicherheitsprozess bereitgestellt oder diese nicht sachgerecht eingesetzt. In letzterem Fall kann dies dazu führen, dass einem übertrieben hohen Sicherheitsniveau in einem Teilbereich schwerwiegende Mängel in einem anderen gegenüberstehen.

Häufig ist auch zu beobachten, dass teure technische Sicherheitslösungen falsch eingesetzt werden und somit unwirksam sind oder sogar selbst zur Gefahrenquelle werden.

2.5. Unzureichende Durchsetzbarkeit von Sicherheitsmaßnahmen

Um ein durchgehendes und angemessenes Sicherheitsniveau zu erreichen, müssen unterschiedliche Zuständigkeitsbereiche innerhalb einer Institution miteinander kooperieren. Fehlende strategische Leitaussagen und unklare Zielsetzungen führen mitunter aber zu unterschiedlichen Interpretationen der Bedeutung von Informationssicherheit. Dies kann zur Folge haben, dass die notwendige Kooperation nicht zustande kommt, etwa weil die Aufgabe „Informationssicherheit" als unnötig angesehen wird oder zumindest keine Priorität hat. Somit könnten Sicherheitsmaßnahmen nicht umgesetzt werden.

2.6. Fehlende Aktualisierung im Sicherheitsprozess

Neue Geschäftsprozesse, Anwendungen und IT-Systeme sowie neue Bedrohungen beeinflussen permanent den Status der Informationssicherheit innerhalb einer Institution. Fehlt ein effektives Revisionskonzept, das auch das Bewusstsein für neue Bedrohungen stärkt, verringert sich das Sicherheitsniveau. Aus der realen Sicherheit wird dann schleichend eine gefährliche Scheinsicherheit.

2.7. Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind, beispielsweise durch ein unzureichendes Sicherheitsmanagement, kann gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern und -partnerinnen verstoßen werden. Welche Gesetze jeweils zu beachten sind, hängt von der Art der Institution beziehungsweise ihrer Geschäftsprozesse und Dienstleistungen ab.

Je nachdem, wo sich die Standorte einer Institution befinden, können auch verschiedene nationale und internationale Vorschriften zu beachten sein. Verfügt eine Institution über unzureichende Kenntnisse hinsichtlich internationaler Gesetzesvorgaben, z. B. zu Datenschutz, Informationspflicht, Insolvenzrecht, Haftung oder Informationszugriff für Dritte, erhöht dies das Risiko entsprechender Verstöße. Dann drohen rechtliche Konsequenzen.

In vielen Branchen ist es üblich, dass Anwendende ihre Zuliefer- und Dienstleistungsunternehmen dazu verpflichten, bestimmte Qualitäts- und Sicherheitsstandards einzuhalten. Verstößt ein Vertragspartner oder -partnerin gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen, Vertragsauflösungen oder sogar den Verlust von Geschäftsbeziehungen nach sich ziehen.

2.8. Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen

Sicherheitsvorfälle können durch ein einzelnes Ereignis oder eine Verkettung unglücklicher Umstände ausgelöst werden. Sie können dazu führen, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und IT-Systemen beeinträchtigt werden. Dies wirkt sich dann schnell negativ auf wesentliche Fachaufgaben und Geschäftsprozesse der betroffenen Institution aus. Auch wenn nicht alle Sicherheitsvorfälle in der Öffentlichkeit bekannt werden, können sie trotzdem zu negativen Auswirkungen in den Beziehungen zu Geschäftspartnern und -partnerinnen sowie Kunden und Kundinnen führen. Auch könnten gesetzliche Vorgaben missachtet werden. Dabei ist es nicht so, dass die schwersten und weitreichendsten Sicherheitsvorfälle durch die größten Sicherheitsschwachstellen ausgelöst wurden. In vielen Fällen führt die Verkettung kleiner Ursachen zu großen Schäden.

2.9. Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

Ein unzureichendes Sicherheitsmanagement kann dazu führen, dass falsche Prioritäten gesetzt werden und nicht an denjenigen Stellen investiert wird, die den größten Mehrwert für die Institution bringen. Dies kann zu folgenden Fehlern führen:

- Es wird in teure Sicherheitslösungen investiert, ohne dass eine Basis an notwendigen organisatorischen Regelungen vorhanden ist. Nicht geklärte Zuständigkeiten und Verantwortlichkeiten können trotz teurer Investitionen zu schweren Sicherheitsvorfällen führen.
- Es wird in den Bereichen einer Institution in Informationssicherheit investiert, die für Informationssicherheit besonders sensibilisiert sind. Andere Bereiche, die vielleicht für die Erfüllung der Fachaufgaben und die Erreichung der Geschäftsziele wichtiger sind, werden aufgrund von knappen Mitteln oder Desinteresse der Verantwortlichen vernachlässigt. Es wird dann unausgewogen in Teilbereiche investiert, während für das Gesamtsystem besonders bedeutsame Sicherheitsrisiken unbeachtet bleiben.
- Durch die einseitige Erhöhung des Schutzes einzelner Grundwerte kann sich der Gesamtschutz sogar verringern, beispielsweise indem eine Verschlüsselung von Informationen die Vertraulichkeit zwar erhöht, aber die Verfügbarkeit verringern kann.
- Ein inhomogener und unkoordinierter Einsatz von Sicherheitsprodukten kann zu hohem finanziellen und personellen Ressourceneinsatz führen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ISMS.1 *Sicherheitsmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Vorgesetzte, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung (B) [Institutionsleitung]

Die Institutionsleitung MUSS die Gesamtverantwortung für Informationssicherheit in der Institution übernehmen. Dies MUSS für alle Beteiligten deutlich erkennbar sein. Die Institutionsleitung MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Institutionsleitung MUSS Informationssicherheit vorleben.

Die Institutionsleitung MUSS die Zuständigkeiten für Informationssicherheit festlegen. Die zuständigen Mitarbeitenden MÜSSEN mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.

Die Institutionsleitung MUSS sich regelmäßig über den Status der Informationssicherheit informieren lassen. Insbesondere MUSS sich die Institutionsleitung über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informieren lassen.

ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie (B) [Institutionsleitung]

Die Institutionsleitung MUSS den Sicherheitsprozess initiieren und etablieren. Dafür MUSS die Institutionsleitung angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festlegen und dokumentieren. Es MÜSSEN konzeptionelle Vorgaben erarbeitet und organisatorische Rahmenbedingungen geschaffen werden, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Geschäftsprozesse des Unternehmens oder Fachaufgaben der Behörde zu ermöglichen.

Die Institutionsleitung MUSS die Sicherheitsstrategie und die Sicherheitsziele tragen und verantworten. Die Institutionsleitung MUSS die Sicherheitsziele und die Sicherheitsstrategie regelmäßig dahingehend überprüfen, ob sie noch aktuell und angemessen sind und wirksam umgesetzt werden können.

ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit (B) [Institutionsleitung]

Die Institutionsleitung MUSS eine übergeordnete Leitlinie zur Informationssicherheit verabschieden. Diese MUSS den Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit beschreiben. Für die Sicherheitsleitlinie MUSS ein klarer Geltungsbereich festgelegt sein. In der Leitlinie zur Informationssicherheit MÜSSEN die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution erläutert werden.

Die Institutionsleitung MUSS die Leitlinie zur Informationssicherheit allen Mitarbeitenden und sonstigen Mitgliedern der Institution bekannt geben. Die Leitlinie zur Informationssicherheit SOLLTE regelmäßig aktualisiert werden.

ISMS.1.A4 Benennung eines oder einer Informationssicherheitsbeauftragten (B) [Institutionsleitung]

Die Institutionsleitung MUSS einen oder eine ISB benennen. Der oder die ISB MUSS die Informationssicherheit in der Institution fördern und den Sicherheitsprozess mitsteuern und koordinieren.

Die Institutionsleitung MUSS den oder die ISB mit angemessenen Ressourcen ausstatten. Die Institutionsleitung MUSS dem oder der ISB die Möglichkeit einräumen, bei Bedarf direkt an sie selbst zu berichten.

Der oder die ISB MUSS bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme frühzeitig beteiligt werden.

ISMS.1.A5 Vertragsgestaltung bei Bestellung eines oder einer externen Informationssicherheitsbeauftragten (B) [Institutionsleitung]

Die Institutionsleitung MUSS einen externen oder eine externe ISB bestellen, wenn die Rolle des oder der ISB nicht durch einen internen Mitarbeitenden besetzt werden kann. Der Vertrag mit einem oder einer externen ISB MUSS alle Aufgaben des oder der ISB sowie die damit verbundenen Rechte und Pflichten umfassen. Der Vertrag MUSS eine geeignete Vertraulichkeitsvereinbarung umfassen. Der Vertrag MUSS eine kontrollierte Beendigung des Vertragsverhältnisses, einschließlich der Übergabe der Aufgaben an die Auftraggebenden, gewährleisten.

ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit (B) [Institutionsleitung]

Eine geeignete übergreifende Organisationsstruktur für Informationssicherheit MUSS vorhanden sein. Dafür MÜSSEN Rollen definiert sein, die konkrete Aufgaben übernehmen, um die Sicherheitsziele zu erreichen. Außerdem MÜSSEN qualifizierte Personen benannt werden, denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen zu übernehmen. Die Aufgaben, Rollen, Verantwortungen und Kompetenzen im Sicherheitsmanagement MÜSSEN nachvollziehbar definiert und zugewiesen sein. Für alle wichtigen Funktionen der Organisation für Informationssicherheit MUSS es wirksame Vertretungsregelungen geben.

Kommunikationswege MÜSSEN geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es MUSS für alle Aufgaben und Rollen festgelegt sein, wer wen informiert und wer bei welchen Aktionen in welchem Umfang informiert werden muss.

Es MUSS regelmäßig geprüft werden, ob die Organisationsstruktur für Informationssicherheit noch angemessen ist oder ob sie an neue Rahmenbedingungen angepasst werden muss.

ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen (B)

Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert werden. Die Sicherheitsmaßnahmen SOLLTEN regelmäßig aktualisiert werden.

ISMS.1.A8 Integration der Mitarbeitenden in den Sicherheitsprozess (B) [Vorgesetzte]

Alle Mitarbeitenden MÜSSEN in den Sicherheitsprozess integriert sein. Hierfür MÜSSEN sie über Hintergründe und die für sie relevanten Gefährdungen informiert sein. Sie MÜSSEN Sicherheitsmaßnahmen kennen und umsetzen, die ihren Arbeitsplatz betreffen.

Alle Mitarbeitenden MÜSSEN in die Lage versetzt werden, Sicherheit aktiv mitzugestalten. Daher SOLLTEN die Mitarbeitenden frühzeitig beteiligt werden, wenn Sicherheitsmaßnahmen zu planen oder organisatorische Regelungen zu gestalten sind.

Bei der Einführung von Sicherheitsrichtlinien und Sicherheitswerkzeugen MÜSSEN die Mitarbeitenden ausreichend informiert sein, wie diese anzuwenden sind.

Die Mitarbeitenden MÜSSEN darüber aufgeklärt werden, welche Konsequenzen eine Verletzung der Sicherheitsvorgaben haben kann.

ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse (B) [Institutionsleitung]

Informationssicherheit MUSS in alle Geschäftsprozesse sowie Fachaufgaben integriert werden. Es MUSS dabei gewährleistet sein, dass nicht nur bei neuen Prozessen und Projekten, sondern auch bei laufenden Aktivitäten alle erforderlichen Sicherheitsaspekte berücksichtigt werden. Der oder die Informationssicherheitsbeauftragte (ISB) MUSS an sicherheitsrelevanten Entscheidungen ausreichend beteiligt werden.

Informationssicherheit SOLLTE außerdem mit anderen Bereichen in der Institution, die sich mit Sicherheit und Risikomanagement beschäftigen, abgestimmt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

ISMS.1.A10 Erstellung eines Sicherheitskonzepts (S)

Für den festgelegten Geltungsbereich (Informationsverbund) SOLLTE ein angemessenes Sicherheitskonzept als das zentrale Dokument im Sicherheitsprozess erstellt werden. Es SOLLTE entschieden werden, ob das Sicherheitskonzept aus einem oder aus mehreren Teilkonzepten bestehen soll, die sukzessive erstellt werden, um zunächst in ausgewählten Bereichen das erforderliche Sicherheitsniveau herzustellen.

Im Sicherheitskonzept MÜSSEN aus den Sicherheitszielen der Institution, dem identifizierten Schutzbedarf und der Risikobewertung konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet werden. Sicherheitsprozess und Sicherheitskonzept MÜSSEN die individuell geltenden Vorschriften und Regelungen berücksichtigen.

Die im Sicherheitskonzept vorgesehenen Maßnahmen MÜSSEN zeitnah in die Praxis umgesetzt werden. Dies MUSS geplant und die Umsetzung MUSS kontrolliert werden.

ISMS.1.A11 Aufrechterhaltung der Informationssicherheit (S)

Der Sicherheitsprozess, die Sicherheitskonzepte, die Leitlinie zur Informationssicherheit und die Organisationsstruktur für Informationssicherheit SOLLTEN regelmäßig auf Wirksamkeit und Angemessenheit überprüft und aktualisiert werden. Dazu SOLLTEN regelmäßig Vollständigkeits- bzw. Aktualisierungsprüfungen des Sicherheitskonzeptes durchgeführt werden.

Ebenso SOLLTEN regelmäßig Sicherheitsrevisionen durchgeführt werden. Dazu SOLLTE geregelt sein, welche Bereiche und Sicherheitsmaßnahmen wann und von wem zu überprüfen sind. Überprüfungen des Sicherheitsniveaus SOLLTEN regelmäßig (mindestens jährlich) sowie anlassbezogen durchgeführt werden.

Die Prüfungen SOLLTEN von qualifizierten und unabhängigen Personen durchgeführt werden. Die Ergebnisse der Überprüfungen SOLLTEN nachvollziehbar dokumentiert sein. Darauf aufbauend SOLLTEN Mängel beseitigt und Korrekturmaßnahmen ergriffen werden.

ISMS.1.A12 Management-Berichte zur Informationssicherheit (S) [Institutionsleitung]

Die Institutionsleitung SOLLTE sich regelmäßig über den Stand der Informationssicherheit informieren, insbesondere über die aktuelle Gefährdungslage sowie die Wirksamkeit und Effizienz des Sicherheitsprozesses. Dazu SOLLTEN Management-Berichte geschrieben werden, welche die wesentlichen relevanten Informationen über den Sicherheitsprozess enthalten, insbesondere über Probleme, Erfolge und Verbesserungsmöglichkeiten. Die Management-Berichte SOLLTEN klar priorisierte Maßnahmenvorschläge enthalten. Die Maßnahmenvorschläge SOLLTEN mit realistischen Abschätzungen zum erwarteten Umsetzungsaufwand versehen sein. Die Management-Berichte SOLLTEN revisionssicher archiviert werden.

Die Management-Entscheidungen über erforderliche Aktionen, den Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen SOLLTEN dokumentiert sein. Die Management-Entscheidungen SOLLTEN revisionssicher archiviert werden.

ISMS.1.A13 Dokumentation des Sicherheitsprozesses (S)

Der Ablauf des Sicherheitsprozesses SOLLTE dokumentiert werden. Wichtige Entscheidungen und die Arbeitsergebnisse der einzelnen Phasen wie Sicherheitskonzept, Richtlinien oder Untersuchungsergebnisse von Sicherheitsvorfällen SOLLTEN ausreichend dokumentiert werden.

Es SOLLTE eine geregelte Vorgehensweise für die Erstellung und Archivierung von Dokumentationen im Rahmen des Sicherheitsprozesses geben. Regelungen SOLLTEN existieren, um die Aktualität und Vertraulichkeit der Dokumentationen zu wahren. Von den vorhandenen Dokumenten SOLLTE die jeweils aktuelle Version kurzfristig zugänglich sein. Außerdem SOLLTEN alle Vorgängerversionen zentral archiviert werden.

ISMS.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit (S)

Die Sicherheitsstrategie SOLLTE wirtschaftliche Aspekte berücksichtigen. Werden Sicherheitsmaßnahmen festgelegt, SOLLTEN die dafür erforderlichen Ressourcen beziffert werden. Die für Informationssicherheit eingeplanten Ressourcen SOLLTEN termingerecht bereitgestellt werden. Bei Arbeitsspitzen oder besonderen Aufgaben SOLLTEN zusätzliche interne Mitarbeitenden eingesetzt oder externe Expertise hinzugezogen werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien (H)

Neben den allgemeinen SOLLTE es auch zielgruppenorientierte Sicherheitsrichtlinien geben, die jeweils bedarfsgerecht die relevanten Sicherheitsthemen abbilden.

ISMS.1.A17 Abschließen von Versicherungen (H)

Es SOLLTE geprüft werden, ob für Restrisiken Versicherungen abgeschlossen werden können. Es SOLLTE regelmäßig überprüft werden, ob die bestehenden Versicherungen der aktuellen Lage entsprechen.

4. Weiterführende Informationen

4.1. Wissenswertes

Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Er ist außerdem kompatibel zum ISO-Standard 27001 und berücksichtigt die Empfehlungen vieler anderer ISO-Standards.

Der BSI-Standard 200-2 bildet die Basis der bewährten BSI-Methodik zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS). Er etabliert drei neue Vorgehensweisen bei der Umsetzung des IT-Grundschutzes. Aufgrund der ähnlichen Struktur der beiden Standards 200-1 und 200-2 können Anwendende sich gut in beiden Dokumenten zurechtfinden.

Die ISO/IEC 27000 (Information security management systems – Overview and vocabulary) gibt einen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge der verschiedenen Normen der ISO/IEC 2700x-Familie. Hier finden sich außerdem die grundlegenden Begriffe und Definitionen für ISMS.

Die ISO/IEC 27001 (Information security management systems – Requirements) ist eine internationale Norm zum Management von Informationssicherheit, die auch eine Zertifizierung ermöglicht.

Die ISO/IEC 27002 (Code of practice for information security controls) unterstützt bei der Auswahl und Umsetzung von den in der ISO/IEC 27001 beschriebenen Maßnahmen, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Institution zu verankern.

ORP: Organisation und Personal

Bundesamt
für Sicherheit in der
Informationstechnik

ORP.1 Organisation

1. Beschreibung

1.1. Einleitung

Jede Institution benötigt eine hierfür zuständige Dienststelle, um den allgemeinen Betrieb zu steuern und zu regeln sowie um Verwaltungsdienstleistungen zu planen, zu organisieren und durchzuführen. Die meisten Institutionen haben hierfür eine Organisationseinheit, die dieses Zusammenspiel der verschiedenen Rollen und Einheiten mit den entsprechenden Geschäftsprozessen und Ressourcen steuert. Bereits auf dieser übergreifenden Ebene sind Aspekte der Informationssicherheit einzubringen und verbindlich festzulegen.

1.2. Zielsetzung

Mit diesem Baustein werden allgemeine und übergreifende Anforderungen im Bereich Organisation aufgeführt, die dazu beitragen, das Niveau der Informationssicherheit zu erhöhen und zu erhalten. In diesem Zusammenhang sind Informationsflüsse, Prozesse, Rollenverteilungen sowie die Aufbau- und Ablauforganisation zu regeln.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.1 *Organisation* ist auf den Informationsverbund mindestens einmal anzuwenden. Wenn Teile des Informationsverbunds einer anderen Organisationseinheit zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Einheit separat angewandt werden.

Der Baustein bildet die übergeordnete Basis, um Informationssicherheit in einer Institution umzusetzen. Er behandelt keine spezifischen Aspekte zu Personal, Schulung von Mitarbeitenden, Verwaltung von Identitäten und Berechtigungen sowie Anforderungsmanagement. Diese Aspekte werden in den Bausteinen ORP.2 *Personal,* ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit,* ORP.4 *Identitäts- und Berechtigungsmanagement* und ORP.5 *Compliance Management (Anforderungsmanagement)* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein ORP.1 *Organisation* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen

Fehlende Regelungen können zu massiven Sicherheitslücken führen, wenn beispielsweise Mitarbeitende nicht wissen, wie sie bei Vorfällen reagieren sollen. Probleme können auch dadurch entstehen, dass Regelungen veraltet, unpraktikabel oder unverständlich formuliert sind.

Die Bedeutung dieser übergreifenden organisatorischen Regelungen nimmt mit der Komplexität der Geschäftsprozesse und dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.

2.2. Nichtbeachtung von Regelungen

Allen Mitarbeitenden müssen die geltenden Regelungen bekannt gemacht werden und zum Nachlesen zur Verfügung stehen. Die Erfahrung zeigt, dass es nicht ausreicht, Sicherheitsregeln lediglich festzulegen. Ihre Kommunika-

tion an die Mitarbeitenden ist elementar wichtig, damit die Vorgaben auch von allen Betroffenen im Arbeitsalltag gelebt werden können.

Werden Regelungen von Mitarbeitenden missachtet, können beispielsweise folgende Sicherheitslücken entstehen:

- Vertrauliche Informationen werden in Hörweite fremder Personen diskutiert, beispielsweise in Pausengesprächen von Besprechungen oder über Mobiltelefonate in öffentlichen Umgebungen.
- Dokumente werden auf einem Webserver veröffentlicht, ohne dass geprüft wurde, ob diese tatsächlich zur Veröffentlichung vorgesehen und freigegeben sind.
- Aufgrund von fehlerhaft administrierten Zugriffsrechten können Mitarbeitende Daten ändern, ohne die Brisanz dieser Integritätsverletzung einschätzen zu können.

2.3. Fehlende, ungeeignete oder inkompatible Betriebsmittel

Wenn benötigte Betriebsmittel in zu geringer Menge vorhanden sind oder nicht termingerecht bereitgestellt werden, können in der Institution Störungen eintreten. Ebenso kann es vorkommen, dass ungeeignete oder sogar inkompatible Betriebsmittel beschafft werden, die infolgedessen nicht eingesetzt werden können.

Beispiel: Der Speicherplatz von Festplatten bei Clients und Servern sowie mobiler Datenträger steigt ständig. Dabei wird häufig vergessen, IT-Komponenten und Datenträger zu beschaffen, die für eine regelmäßige Datensicherung ausreichend Kapazität bieten.

Ebenso muss die Funktionsfähigkeit der eingesetzten Betriebsmittel gewährleistet sein. Wenn Wartungsarbeiten nicht oder nur unzureichend durchgeführt werden, können daraus hohe Schäden entstehen.

Beispiele:

- Die Kapazität der Batterien einer unterbrechungsfreien Stromversorgung (USV-Anlage) wurde nicht rechtzeitig überprüft. Ist die Kapazität bzw. der Säuregehalt zu gering, kann die USV-Anlage einen Stromausfall nicht mehr ausreichend lange überbrücken.
- Die Feuerlöscher wurden nicht rechtzeitig gewartet und verfügen deshalb nicht mehr über einen ausreichenden Druck. Ihre Löschleistung ist somit im Brandfall nicht mehr gewährleistet.

2.4. Gefährdung durch Institutionsfremde

Bei Institutionsfremden kann grundsätzlich nicht vorausgesetzt werden, dass sie mit ihnen zugänglichen Informationen und der Informationstechnik entsprechend den Vorgaben der besuchten Institution umgehen.

Besuchende, Reinigungs- und Fremdpersonal können interne Informationen, Geschäftsprozesse und IT-Systeme auf verschiedene Arten gefährden, angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen über den Versuch des „Spielens“ an IT-Systemen bis hin zum Diebstahl von Unterlagen oder IT-Komponenten.

Beispiele:

- Unbegleitete Besuchende können auf Unterlagen und Datenträger zugreifen oder Zugang zu Geräten haben, diese beschädigen oder schützenswerte Informationen ausspähen.
- Reinigungskräfte können versehentlich Steckverbindungen lösen, Wasser in Geräte laufen lassen, Unterlagen verlegen oder mit dem Abfall entsorgen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.1 *Organisation* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Zentrale Verwaltung
Weitere Zuständigkeiten	Mitarbeitende, Benutzende, IT-Betrieb, Haustechnik, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

ORP.1.A1 Festlegung von Verantwortlichkeiten und Regelungen (B) [Institutionsleitung]

Innerhalb einer Institution MÜSSEN alle relevanten Aufgaben und Funktionen klar definiert und voneinander abgegrenzt sein. Es MÜSSEN verbindliche Regelungen für die Informationssicherheit für die verschiedenen betrieblichen Aspekte übergreifend festgelegt werden. Die Organisationsstrukturen sowie verbindliche Regelungen MÜSSEN anlassbezogen überarbeitet werden. Die Änderungen MÜSSEN allen Mitarbeitenden bekannt gegeben werden.

ORP.1.A2 Zuweisung der Zuständigkeiten (B) [Institutionsleitung]

Für alle Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen MUSS festgelegt werden, wer für diese und deren Sicherheit zuständig ist. Alle Mitarbeitenden MÜSSEN darüber informiert sein, insbesondere wofür sie zuständig sind und welche damit verbundenen Aufgaben sie wahrnehmen.

ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonen (B) [Mitarbeitende]

Institutionsfremde Personen MÜSSEN von Mitarbeitenden zu den Räumen begleitet werden. Die Mitarbeitenden der Institution MÜSSEN institutionsfremde Personen in sensiblen Bereichen beaufsichtigen. Die Mitarbeitenden SOLLTEN dazu angehalten werden, institutionsfremde Personen in den Räumen der Institution nicht unbeaufsichtigt zu lassen.

ORP.1.A4 Funktionstrennung zwischen unvereinbaren Aufgaben (B)

Die Aufgaben und die hierfür erforderlichen Rollen und Funktionen MÜSSEN so strukturiert sein, dass unvereinbare Aufgaben wie operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden. Für unvereinbare Funktionen MUSS eine Funktionstrennung festgelegt und dokumentiert sein. Auch Vertreter MÜSSEN der Funktionstrennung unterliegen.

ORP.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

ORP.1.A15 Ansprechperson zu Informationssicherheitsfragen (B)

In jeder Institution MUSS es Ansprechpersonen für Sicherheitsfragen geben, die sowohl scheinbar einfache wie auch komplexe oder technische Fragen beantworten können. Die Ansprechpersonen MÜSSEN allen Mitarbeitenden der Institution bekannt sein. Diesbezügliche Informationen MÜSSEN in der Institution für alle verfügbar und leicht zugänglich sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.1.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.1.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.1.A8 Betriebsmittel- und Geräteverwaltung (S) [IT-Betrieb]

Alle Geräte und Betriebsmittel, die Einfluss auf die Informationssicherheit haben und die zur Aufgabenerfüllung und zur Einhaltung der Sicherheitsanforderungen erforderlich sind, SOLLTEN in ausreichender Menge vorhanden sein. Es SOLLTE geeignete Prüf- und Genehmigungsverfahren vor Einsatz der Geräte und Betriebsmittel geben. Geräte und Betriebsmittel SOLLTEN in geeigneten Bestandsverzeichnissen aufgelistet werden. Um den Missbrauch von Daten zu verhindern, SOLLTE die zuverlässige Löschung oder Vernichtung von Geräten und Betriebsmitteln geregelt sein (siehe hierzu CON.6 *Löschen und Vernichten*).

ORP.1.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.1.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.1.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.1.A13 Sicherheit bei Umzügen (S) [IT-Betrieb, Haustechnik]

Vor einem Umzug SOLLTEN frühzeitig Sicherheitsrichtlinien erarbeitet bzw. aktualisiert werden. Alle Mitarbeitenden SOLLTEN über die vor, während und nach dem Umzug relevanten Sicherheitsmaßnahmen informiert werden. Nach dem Umzug SOLLTE überprüft werden, ob das transportierte Umzugsgut vollständig und unbeschädigt bzw. unverändert angekommen ist.

ORP.1.A16 Richtlinie zur sicheren IT-Nutzung (S) [Benutzende]

Es SOLLTE eine Richtlinie erstellt werden, in der für alle Mitarbeitenden transparent beschrieben wird, welche Rahmenbedingungen bei der IT-Nutzung eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie SOLLTE folgende Punkte abdecken:

- Sicherheitsziele der Institution,
- wichtige Begriffe,
- Aufgaben und Rollen mit Bezug zur Informationssicherheit,
- Ansprechperson zu Fragen der Informationssicherheit sowie
- von den Mitarbeitenden umzusetzende und einzuhaltende Sicherheitsmaßnahmen.

Die Richtlinie SOLLTE allen Benutzenden zur Kenntnis gegeben werden. Jeder neue Benutzende SOLLTE die Kenntnisnahme und Beachtung der Richtlinie schriftlich bestätigen, bevor er die Informationstechnik nutzen darf. Benutzende SOLLTEN die Richtlinie regelmäßig oder nach größeren Änderungen erneut bestätigen. Die Richtlinie sollte zum Nachlesen für alle Mitarbeitenden frei zugänglich abgelegt werden, beispielsweise im Intranet.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

ORP.1.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.1.A17 Mitführverbot von Mobiltelefonen (H)

Mobiltelefone SOLLTEN NICHT zu vertraulichen Besprechungen und Gesprächen mitgeführt werden. Falls erforderlich, SOLLTE dies durch Mobilfunk-Detektoren überprüft werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein ORP.1 *Organisation* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

ORP.2 Personal

1. Beschreibung

1.1. Einleitung

Das Personal eines Unternehmens bzw. einer Behörde hat einen entscheidenden Anteil am Erfolg oder Misserfolg der Institution. Die Mitarbeitenden haben dabei die wichtige Aufgabe, Informationssicherheit umzusetzen. Die aufwendigsten Sicherheitsvorkehrungen können ins Leere laufen, wenn sie im Arbeitsalltag nicht gelebt werden. Die elementare Bedeutung von Informationssicherheit für eine Institution und ihre Geschäftsprozesse muss daher für das Personal transparent und nachvollziehbar aufbereitet sein.

1.2. Zielsetzung

Ziel dieses Bausteins ist es aufzuzeigen, welche „personellen" Sicherheitsmaßnahmen die Personalabteilung oder Vorgesetzten ergreifen müssen, damit die Mitarbeitenden verantwortungsbewusst mit den Informationen der Institution umgehen und sich so gemäß den Vorgaben verhalten.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.2 *Personal* ist für den Informationsverbund einmal anzuwenden.

Der Baustein beschäftigt sich mit den Anforderungen, die durch die Personalabteilung oder die Vorgesetzten einer Institution zu beachten und zu erfüllen sind. Personelle Anforderungen, die an eine bestimmte Funktion gebunden sind, wie z. B. die Ernennung des oder der Systemadministrierenden eines LAN, werden in den Bausteinen angeführt, die sich mit dem jeweiligen Themengebiet beschäftigen. Der Baustein ORP.2 *Personal* behandelt keine spezifischen Aspekte zu Schulung von Mitarbeitenden oder Verwaltung von Identitäten und Berechtigungen. Diese Aspekte werden in den Bausteinen ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und ORP.4 I*dentitäts- und Berechtigungsmanagement* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein ORP.2 *Personal* von besonderer Bedeutung.

2.1. Personalausfall

Der Ausfall von Personal kann dazu führen, dass bestimmte Aufgaben nicht mehr oder nicht zeitnah wahrgenommen werden können.

2.2. Unzureichende Kenntnis über Regelungen

Regelungen festzulegen allein garantiert noch nicht, dass diese auch beachtet werden und der Betrieb störungsfrei funktionieren kann. Allen Mitarbeitenden müssen die geltenden Regelungen bekannt sein, vor allem den Funktionsträgern. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, sollte sich nicht mit den Aussagen entschuldigen lassen: „Ich habe nicht gewusst, dass ich dafür zuständig bin." oder „Ich habe nicht gewusst, wie ich zu verfahren hatte."

2.3. Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass es in Institutionen zwar viele organisatorische und technische Sicherheitsverfahren gibt, diese jedoch durch den sorglosen Umgang der Mitarbeitenden wieder umgangen werden. Ein typisches Beispiel hierfür sind etwa Zettel am Monitor, auf denen Zugangspasswörter notiert sind.

2.4. Unzureichende Qualifikationen der Mitarbeitenden

Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten. Sind die verantwortlichen Mitarbeitenden nicht ausreichend qualifiziert, sensibilisiert und geschult, haben sie z. B. einen veralteten Wissensstand für ihre Aufgabenerfüllung, könnten sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so Angriffe unerkannt bleiben. Auch wenn die Mitarbeitenden ausreichend für die Belange der Informationssicherheit qualifiziert, sensibilisiert bzw. geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen. In manchen Situationen, wie bei Personalmangel oder Kündigungen, kann es passieren, dass Mitarbeitende die Aufgaben anderer Mitarbeitenden vorübergehend übernehmen müssen. Hierbei können Fehler entstehen, wenn Mitarbeitende nicht die notwendigen Qualifikationen haben oder unzureichend geschult sind, um die Aufgabe zu übernehmen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.2 *Personal* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Personalabteilung
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeitender (B) [Vorgesetzte]

Die Personalabteilung sowie die Vorgesetzten MÜSSEN dafür sorgen, dass Mitarbeitende zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet werden. Die Mitarbeitenden MÜSSEN über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden. Eine Checkliste und ein direkter Ansprechpartner oder Ansprechpartnerin („Pate oder Patin“) kann hierbei hilfreich sein und SOLLTE etabliert werden.

ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitenden (B) [Vorgesetzte, IT-Betrieb]

Verlassen Mitarbeitende die Institution, MUSS der oder die Nachfolgende rechtzeitig eingewiesen werden. Dies SOLLTE idealerweise durch den oder die ausscheidenden Mitarbeitenden erfolgen. Ist eine direkte Übergabe nicht möglich, MUSS von den ausscheidenden Mitarbeitenden eine ausführliche Dokumentation angefertigt werden.

Außerdem MÜSSEN von ausscheidenden Mitarbeitenden alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen eingezogen werden.

Vor der Verabschiedung MUSS noch einmal auf Verschwiegenheitsverpflichtungen hingewiesen werden. Es SOLLTE besonders darauf geachtet werden, dass keine Interessenkonflikte auftreten. Um nach einem Stellenwechsel Interessenkonflikte zu vermeiden, SOLLTEN Konkurrenzverbote und Karenzzeiten vereinbart werden.

Weiterhin MÜSSEN Notfall- und andere Ablaufpläne aktualisiert werden. Alle betroffenen Stellen innerhalb der Institution, wie z. B. das Sicherheitspersonal oder die IT-Abteilung, MÜSSEN über das Ausscheiden des oder der Mitarbeitenden informiert werden. Damit alle verbundenen Aufgaben, die beim Ausscheiden des oder der Mitarbeitenden anfallen, erledigt werden, SOLLTE hier ebenfalls eine Checkliste angelegt werden. Zudem SOLLTE es einen festen Ansprechpartner oder Ansprechpartnerin der Personalabteilung geben, der den Weggang von Mitarbeitenden begleitet.

ORP.2.A3 Festlegung von Vertretungsregelungen (B) [Vorgesetzte]

Die Vorgesetzten MÜSSEN dafür sorgen, dass im laufenden Betrieb Vertretungsregelungen umgesetzt werden. Dafür MUSS sichergestellt werden, dass es für alle wesentlichen Geschäftsprozesse und Aufgaben praktikable Vertretungsregelungen gibt. Bei diesen Regelungen MUSS der Aufgabenumfang der Vertretung im Vorfeld klar definiert werden. Es MUSS sichergestellt werden, dass die Vertretung über das dafür nötige Wissen verfügt. Ist dies nicht der Fall, MUSS überprüft werden, wie der Vertretenden zu schulen ist oder ob es ausreicht, den aktuellen Verfahrens- oder Projektstand ausreichend zu dokumentieren. Ist es im Ausnahmefall nicht möglich, für einzelne Mitarbeitende einen kompetenten Vertretenden zu benennen oder zu schulen, MUSS frühzeitig entschieden werden, ob externes Personal dafür hinzugezogen werden kann.

ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal (B)

Wird externes Personal beschäftigt, MUSS dieses wie alle eigenen Mitarbeitenden dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Fremdpersonal, das kurzfristig oder einmalig eingesetzt wird, MUSS in sicherheitsrelevanten Bereichen beaufsichtigt werden. Bei längerfristig beschäftigtem Fremdpersonal MUSS dieses wie die eigenen Mitarbeitenden in seine Aufgaben eingewiesen werden. Auch für diese Mitarbeitende MUSS eine Vertretungsregelung eingeführt werden. Verlässt das Fremdpersonal die Institution, MÜSSEN Arbeitsergebnisse wie bei eigenem Personal geregelt übergeben und eventuell ausgehändigte Zugangsberechtigungen zurückgegeben werden.

ORP.2.A5 Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal (B)

Bevor externe Personen Zugang und Zugriff zu vertraulichen Informationen erhalten, MÜSSEN mit ihnen Vertraulichkeitsvereinbarungen in schriftlicher Form geschlossen werden. In diesen Vertraulichkeitsvereinbarungen MÜSSEN alle wichtigen Aspekte zum Schutz von institutionsinternen Informationen berücksichtigt werden.

ORP.2.A14 Aufgaben und Zuständigkeiten von Mitarbeitenden (B) [Vorgesetzte]

Alle Mitarbeitenden MÜSSEN dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Den Mitarbeitenden MUSS der rechtliche Rahmen ihre Tätigkeit bekannt sein. Die Aufgaben und Zuständigkeiten von Mitarbeitenden MÜSSEN in geeigneter Weise dokumentiert sein. Außerdem MÜSSEN alle Mitarbeitenden darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind. Den Mitarbeitenden MUSS bewusst gemacht werden, die Informationssicherheit der Institution auch außerhalb der Arbeitszeit und außerhalb des Betriebsgeländes zu schützen.

ORP.2.A15 Qualifikation des Personals (B) [Vorgesetzte]

Mitarbeitende MÜSSEN regelmäßig geschult bzw. weitergebildet werden. In allen Bereichen MUSS sichergestellt werden, dass kein Mitarbeitende mit veralteten Wissensstand arbeitet. Weiterhin SOLLTE den Mitarbeitenden während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.

Werden Stellen besetzt, MÜSSEN die erforderlichen Qualifikationen und Fähigkeiten genau formuliert sein. Anschließend SOLLTE geprüft werden, ob diese bei den Bewerbenden für die Stelle tatsächlich vorhanden sind. Es MUSS sichergestellt sein, dass Stellen nur von Mitarbeitenden besetzt werden, für die sie qualifiziert sind.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.2.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.2.A7 Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden (S)

Neue Mitarbeitende SOLLTEN auf ihre Vertrauenswürdigkeit hin überprüft werden, bevor sie eingestellt werden. Soweit möglich, SOLLTEN alle an der Personalauswahl Beteiligten kontrollieren, ob die Angaben der Bewerbenden, die relevant für die Einschätzung ihrer Vertrauenswürdigkeit sind, glaubhaft sind. Insbesondere SOLLTE sorgfältig geprüft werden, ob der vorgelegte Lebenslauf korrekt, plausibel und vollständig ist. Dabei SOLLTEN auffällig erscheinende Angaben überprüft werden.

ORP.2.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

ORP.2.A11 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.2.A12 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.2.A13 Sicherheitsüberprüfung (H)

Im Hochsicherheitsbereich SOLLTE eine zusätzliche Sicherheitsüberprüfung zusätzlich zur grundlegenden Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden durchgeführt werden.

Arbeiten Mitarbeitende mit nach dem Geheimschutz klassifizierten Verschlusssachen, SOLLTEN sich die entsprechenden Mitarbeitenden einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Diesbezüglich SOLLTE der oder die Informationssicherheitsbeauftragte den Geheimschutzbeauftragten oder die Geheimschutzbeauftragte bzw. Sicherheitsbevollmächtigten oder Sicherheitsbevollmächtigte der Institution einbeziehen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology – Security techniques – Information security management systems – Requirements“ im Anhang A.7 Personalsicherheit Vorgaben für die Personalsicherheit.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel PM: People Management Vorgaben für die Personalsicherheit.

Bundesamt
für Sicherheit in der
Informationstechnik

ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

1. Beschreibung

1.1. Einleitung

Mitarbeitende sind ein wichtiger Erfolgsfaktor für ein hohes Maß an Informationssicherheit in einer Institution. Daher ist es wichtig, dass sie die Sicherheitsziele kennen, die Sicherheitsmaßnahmen verständlich sind und jeder einzelne Mitarbeitende bereit ist, diese umzusetzen. Die Voraussetzung dafür ist, dass es ein Sicherheitsbewusstsein innerhalb der Institution gibt. Darüber hinaus sollte eine Sicherheitskultur aufgebaut und im Arbeitsalltag mit Leben gefüllt werden.

Mitarbeitende müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Ihnen muss bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollen.

1.2. Zielsetzung

In diesem Baustein wird beschrieben, wie ein effektives Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit aufgebaut und aufrechterhalten werden kann. Ziel des Programms ist es, die Wahrnehmung der Mitarbeitenden für Sicherheitsrisiken zu schärfen und ihnen die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten zu vermitteln.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* ist für den Informationsverbund einmal anzuwenden.

Dieser Baustein formuliert Anforderungen an die Sensibilisierung und Schulung zur Informationssicherheit, die das Arbeitsumfeld in der Institution, den Telearbeitsplatz und die mobile Arbeit betreffen.

Der Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* beschreibt die prozessualen, technischen, methodischen und organisatorischen Anforderungen an die Sensibilisierung und Schulung von Informationssicherheit. Weitere Schulungsthemen werden durch die Personalabteilung oder das Weiterbildungsmanagement geplant, gestaltet und durchgeführt.

In vielen der anderen IT-Grundschutz-Bausteine werden konkrete Schulungsinhalte zu den dort betrachteten Themen beschrieben. Der vorliegende Baustein beschäftigt sich damit, wie in den Bereichen Sensibilisierung und Schulung zur Informationssicherheit ein planvolles Vorgehen effizient gestaltet werden kann.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* von besonderer Bedeutung.

2.1. Unzureichende Kenntnis über Regelungen

Regelungen zur Informationssicherheit lediglich festzulegen, garantiert nicht, dass sie auch beachtet werden. Allen Mitarbeitenden, insbesondere die in Funktion gewählten Personen, müssen die geltenden Regelungen auch bekannt sein. Bei vielen Sicherheitsvorfällen ist die Nichtbeachtung von Regelungen zwar nicht der alleinige Auslöser

des Vorfalls, aber mit ein Grund dafür, dass er auftritt. Sicherheitslücken aufgrund unzureichender Kenntnisse über Regelungen können die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, mit denen gearbeitet wird, gefährden. Die Aufgabenerfüllung und die Abwicklung von Geschäftsprozessen und Fachaufgaben können dadurch eingeschränkt werden.

2.2. Unzureichende Sensibilisierung für Informationssicherheit

Die Erfahrung zeigt, dass es nicht genügt, Sicherheitsmaßnahmen lediglich anzuordnen. Die Mitarbeitenden sollten die Bedeutung und den Zweck der Maßnahmen kennen, da diese ansonsten im Arbeitsalltag ignoriert werden könnten. Werden Mitarbeitende unzureichend zu Informationssicherheitsthemen sensibilisiert, können die Sicherheitskultur, die Sicherheitsziele und die Sicherheitsstrategie der Institution gefährdet sein.

2.3. Unwirksame Aktivitäten zur Sensibilisierung und Schulung

Nicht immer sind die zur Sensibilisierung und Schulung durchgeführten Aktivitäten so erfolgreich wie gewünscht. Ursachen dafür können sein:

- eine fehlende Management-Unterstützung,
- unklare Ziele,
- schlechte Planung,
- mangelnde Erfolgskontrolle,
- fehlende Kontinuität sowie
- zu geringe finanzielle oder personelle Ressourcen.

Werden keine geeigneten Maßnahmen ergriffen, um den Erfolg der durchgeführten Aktivitäten sicherzustellen, kann das Ziel der jeweiligen Schulungsaktivität häufig nicht erreicht werden. Wenn die Institution unzureichende Aktivitäten zur Sensibilisierung und Schulung der Mitarbeitenden durchführt, können Aspekte der Informationssicherheit gefährdet sein, was direkt die Aufgabenerfüllung einschränkt.

2.4. Unzureichende Schulung der Mitarbeitenden zu Sicherheitsfunktionen

Häufig wenden Mitarbeitende neu eingeführte Sicherheitsprogramme und -funktionen deswegen nicht an, weil sie nicht wissen, wie sie bedient werden, und sie es als zu zeitaufwendig ansehen, sich im täglichen Arbeitsablauf selbstständig darin einzuarbeiten. Darüber hinaus können fehlende Schulungen nach Einführung einer neuen Software dazu führen, dass Mitarbeitende diese falsch bedienen oder falsch konfigurieren und Arbeitsabläufe sich unnötig verzögern. Daher reicht die Beschaffung und Installation einer (Sicherheits-)Software nicht aus. Besonders bei kritischen IT-Systemen und -Anwendungen kann eine Fehlbedienung existenzbedrohende Auswirkungen nach sich ziehen.

2.5. Nicht erkannte Sicherheitsvorfälle

Im täglichen Betrieb von IT- und ICS-Komponenten können viele Störungen und Fehler auftreten. Dabei könnten Sicherheitsvorfälle durch das Personal nicht als solche identifiziert werden und auch Cyber-Angriffe bzw. Angriffsversuche unerkannt bleiben. Sicherheitsvorfälle und technische Fehler sind mitunter nicht einfach zu unterscheiden. Werden Benutzende und Administrierende nicht gezielt darin geschult und dafür sensibilisiert, Sicherheitsvorfälle zu erkennen und auf diese angemessen zu reagieren, können Sicherheitslücken unentdeckt bleiben und ausgenutzt werden. Falls Sicherheitsvorfälle zu spät oder gar nicht erkannt werden, können wirksame Gegenmaßnahmen nicht rechtzeitig ergriffen werden. Kleine Sicherheitslücken der Institution können zu kritischen Gefährdungen für die Integrität, Vertraulichkeit und Verfügbarkeit heranwachsen. Dies kann Geschäftsprozesse behindern, finanzielle Schäden hervorrufen oder regulatorische und gesetzliche Sanktionen nach sich ziehen.

2.6. Nichtbeachtung von Sicherheitsmaßnahmen

Verschiedenste Gründen, wie Unachtsamkeit oder Hektik, können dazu führen, dass beispielsweise vertrauliche Dokumente an Arbeitsplätzen offen herumliegen oder E-Mails nicht verschlüsselt werden. Durch solche vermeintlich kleinen Nachlässigkeiten können Schäden entstehen, die gut geschulten Mitarbeitenden in der Regel nicht passieren.

2.7. Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen zwar eine Vielzahl von organisatorischen und technischen Sicherheitsverfahren festgelegt sind, diese jedoch durch den sorglosen Umgang der Mitarbeitenden umgangen werden. Ein typisches Beispiel hierfür sind die fast schon berühmten Zettel am Monitor, auf denen Zugangspasswörter notiert sind. Ebenso schützt eine Festplattenverschlüsselung einen Laptop unterwegs nicht davor, dass vertrauliche Informationen etwa vom Sitznachbarn im Zug einfach mitgelesen werden können. Die besten technischen Sicherheitslösungen helfen nicht, wenn Ausdrucke mit vertraulichen Informationen am Drucker liegenbleiben oder in frei zugänglichen Altpapiercontainern landen.

Wenn die Mitarbeitenden sorglos mit Informationen umgehen, werden festgelegte Prozesse der Informationssicherheit unwirksam. Unbefugte könnten z. B. Nachlässigkeiten im Umgang mit Informationen ausnutzen, um gezielt Wirtschaftsspionage zu betreiben.

2.8. Fehlende Akzeptanz von Informationssicherheitsvorgaben

Es kann unterschiedliche Gründe dafür geben, warum Mitarbeitende die Vorgaben zur Informationssicherheit nicht umsetzen. Dazu zählen beispielsweise eine fehlende Sicherheitskultur der Institution oder eine fehlende Vorbildfunktion durch die Institutionsleitung. Aber auch übertriebene Sicherheitsanforderungen können dazu führen, dass Mitarbeitende Sicherheitsmaßnahmen ablehnen. Probleme können außerdem dadurch entstehen, dass bestimmte Berechtigungen oder auch die Ausstattung mit bestimmter Hard- oder Software als Statussymbol gesehen werden. Einschränkungen in diesen Bereichen können auf großen Widerstand stoßen.

2.9. Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugriff auf Informationen oder Zugang zu IT-Systemen durch „Aushorchen" von Mitarbeitenden zu erlangen. Beim Social Engineering baut der oder die Angreifende meistens einen direkten Kontakt zu einem Opfer auf, z. B. per Telefon, E-Mail oder auch über Soziale Netzwerke. Angriffe über Social Engineering sind häufig mehrstufig. Indem der oder die Angreifende Insiderwissen vorgibt und gleichzeitig an die Hilfsbereitschaft appelliert, kann er oder sie sein oder ihr Wissen in weiteren Schritten ausbauen. Wenn Mitarbeitende für diese Art von Angriffen nicht ausreichend sensibilisiert sind, könnten sie durch geschickte Kommunikation so manipuliert werden, dass sie unzulässig handeln. Dies kann dazu führen, dass sie interne Informationen weitergeben, ihre IT-Systeme sich mit Schadsoftware infizieren oder sogar Geld an angebliche Geschäftspartner und Geschäftspartnerin überweisen.

So wird beispielsweise beim sogenannten „CEO Fraud" Mitarbeitenden, die Geld im Namen der Institution transferieren dürfen, ein fiktiver Auftrag der Leitung vorgegaukelt. Sie sollen für ein angeblich dringendes und vertrauliches Geschäft Transaktionen durchführen, die für das weitere Bestehen der Institution äußerst wichtig sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte, Personalabteilung, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

ORP.3.A1 Sensibilisierung der Institutionsleitung für Informationssicherheit (B) [Vorgesetzte, Institutionsleitung]

Die Institutionsleitung MUSS ausreichend für Sicherheitsfragen sensibilisiert werden. Die Sicherheitskampagnen und Schulungsmaßnahmen MÜSSEN von der Institutionsleitung unterstützt werden. Vor dem Beginn eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit MUSS die Unterstützung der Institutionsleitung eingeholt werden.

Alle Vorgesetzten MÜSSEN die Informationssicherheit unterstützen, indem sie mit gutem Beispiel vorangehen. Führungskräfte MÜSSEN die Sicherheitsvorgaben umsetzen. Hierüber hinaus MÜSSEN sie ihre Mitarbeitenden auf deren Einhaltung hinweisen.

ORP.3.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

ORP.3.A3 Einweisung des Personals in den sicheren Umgang mit IT (B) [Vorgesetzte, Personalabteilung, IT-Betrieb]

Alle Mitarbeitenden und externen Benutzenden MÜSSEN in den sicheren Umgang mit IT-, ICS- und IoT-Komponenten eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeitszusammenhänge relevant ist. Dafür MÜSSEN verbindliche, verständliche und aktuelle Richtlinien zur Nutzung der jeweiligen Komponenten zur Verfügung stehen. Werden IT-, ICS- oder IoT-Systeme oder -Dienste in einer Weise benutzt, die den Interessen der Institution widersprechen, MUSS dies kommuniziert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

ORP.3.A4 Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit (S)

Sensibilisierungs- und Schulungsprogramme zur Informationssicherheit SOLLTEN sich an den jeweiligen Zielgruppen orientieren. Dazu SOLLTE eine Zielgruppenanalyse durchgeführt werden. Hierbei SOLLTEN Schulungsmaßnahmen auf die speziellen Anforderungen und unterschiedlichen Hintergründe fokussiert werden können.

Es SOLLTE ein zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erstellt werden. Dieses Schulungsprogramm SOLLTE den Mitarbeitenden alle Informationen und Fähigkeiten vermitteln, die erforderlich sind, um in der Institution geltende Sicherheitsregelungen und -maßnahmen umsetzen zu können. Es SOLLTE regelmäßig überprüft und aktualisiert werden.

ORP.3.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit (S)

Alle Mitarbeitenden SOLLTEN entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.

ORP.3.A7 Schulung zur Vorgehensweise nach IT-Grundschutz (S)

Informationssicherheitsbeauftragte SOLLTEN mit dem IT-Grundschutz vertraut sein. Wurde ein Schulungsbedarf identifiziert, SOLLTE eine geeignete IT-Grundschutz-Schulung geplant werden. Für die Planung einer Schulung SOLLTE der Online-Kurs des BSI zum IT-Grundschutz berücksichtigt werden. Innerhalb der Schulung SOLLTE die Vorgehensweise anhand praxisnaher Beispiele geübt werden. Es SOLLTE geprüft werden, ob der oder die Informationssicherheitsbeauftragte sich zu einem BSI IT-Grundschutz-Praktiker qualifizieren lassen sollten.